CS 2204-01 Communications and Networking

Instructor: Professor Sharon Sisitzky

Name: Anonymos

Written Assignment Unit 3

**1. What do you understand by The Hidden Node Problem? Describe 2 different spatial configurations which exemplify this issue.**

The hidden node problem is a unique problem that occurs in wireless network communications. This problem refers to a situation in which one node in the network is unable to detect the transmissions of another node. This makes communication collisions more likely and reduces the efficiency of the network.

Here are two different spatial arrangements that illustrate the hidden node problem

Linear Arrangement: In this arrangement, nodes A, B, and C are aligned in a straight line; A and C are too far apart to communicate directly, and B is in the middle; A and B can communicate with each other, and B and C can communicate with each other, but A and C cannot communicate directly, so C starts sending to B while A is sending to B If this happens, there is a possibility that A and C's transmissions will collide at B. In this case, A and C will not be able to communicate with each other. In this case, A and C attempting to send to B simultaneously without knowing each other's presence causes the hidden node problem.

Circular Arrangement: In this arrangement, nodes are arranged in a circle and one node may not be able to directly detect the transmission of a node on the other side of the circle. For example, suppose nodes A, B, and C are each equally spaced around the circle; when A is transmitting to B, C may start transmitting to B as well. However, since A and C cannot directly detect each other's transmissions, there is a risk of transmission collisions at B, which represents a hidden node problem.

To mitigate these problems, wireless networks use techniques such as the RTS/CTS (Request to Send/Clear to Send) mechanism. This allows all nodes in the network to detect each other's transmissions and avoid communication collisions.

**2. What is the 4B/5B encoding for the 3-byte (ASCII) string “Sun”?**

4B/5B encoding is an encoding method used in data communications that converts 4-bit data into a 5-bit code. This makes it easier to keep signals synchronized and reduces transmission errors. To convert the ASCII string "Sun" into 4B/5B encoding as 3 bytes of data, the string is first converted into binary form, and then each 4 bits is converted into the corresponding 5-bit code.

In ASCII code, "S" is 83 (decimal), "u" is 117 (decimal), and "n" is 110 (decimal). These are converted to binary format and then 4B/5B encoding is applied. The following steps are used to perform the calculations.

The binary representation of the ASCII string "Sun" is

S: 01010011

u: 01110101

n: 01101110

**3. What is the 16-bit internet checksum for the 3-byte binary message 00110001 00110010 00110011?**

The process first sums all bytes (or two-byte words) and, if an overflow occurs, wraps around the overflow and adds it again. Finally, a checksum is obtained by taking a bitwise inversion of the sum. To perform this calculation, the 3-byte binary message is first divided into 16-bit words, which are then summed to compute the checksum.

The 16-bit Internet checksum of the 3-byte binary message "00110001 00110010 00110011" is 39885 in decimal and "1001101111001101" in binary. This checksum is used by the receiver to verify the correctness of the message.

**4. Suppose a message is 11011000. What is the CRC checksum using the polynomial corresponding to 1011 to give a 3-bit answer? (Show the solution steps, not just the answer).**

The calculation of the CRC (Cyclic Redundancy Check) checksum is a powerful method for detecting data transmission errors. In this problem, the 3-bit CRC checksum is calculated using the message "11011000" and the polynomial "1011". The calculation process is similar to polynomial division and is done in binary. Here, the CRC checksum is calculated through specific steps.

The CRC checksum calculated using the polynomial "1011" for the message "11011000" is "011". The calculation process adds zeros to the message by the length of the polynomial -1 (2 bits in this case), then performs a binary division (using the XOR operation) to obtain the final remainder as the checksum. This checksum is used to verify the correctness of the data.

**5. What is Time Domain Reflectometry?**

Time Domain Reflectometry (TDR) is a technique used to detect faults and characteristics of cables and conductors. In this technique, an electrical signal is sent to a cable and the reflected wave is analyzed to determine the length of the cable, the location of breaks, poor connections, and impedance changes in the cable.

The principle of TDR is similar to radar technology. Specific pulses are sent to the cable and the reflected pulses are received within the cable. Reflections can be caused by cable damage, mismatched terminations, or other anomalies. By measuring the time delay and amplitude of the reflected pulses, the location and nature of the anomaly can be determined.

TDR is a nondestructive test and can be used even when cables are buried or difficult to access. Useful for diagnosing many types of cables, including telephone lines, coaxial cables, and power cables, TDR is a valuable tool in cable maintenance and fault diagnosis.

Word-Count: 867

References

Dordal, P. (2019). *An introduction to computer networks.*

(n.d.). *Computer networks.*